UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,721	11/17/2003	Sunil K. Srivastava	50325-0855	4990

29989 7590 01/25/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/715,721	SRIVASTAVA, SUNIL K.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/27/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 30 September 2005 has been noted and made of record.

2. Claims 1-28 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see pages 12- 15, filed 30 September 2005, with respect to claims 1-10 and 26-28 have been fully considered and are persuasive. The rejection of claims 1-10 and 26-28 has been withdrawn.

4. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as receiving a third public key valued from a third node that seeks to join the first network communication entity and creating a second shared secret key valued based on the collective public key value and the third public key value, are not recited in the remaining rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

5. See further rejections that follow.

Claim Rejections

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 11-15, 17-20, and 22-25 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,668,877 to Aziz, hereinafter Aziz.

8. As per claim 11, Aziz teaches a method for establishing a secure communication session among a first node of a network and one or more other nodes that joined in a first network

communication entity, using a group shared secret key value, each of the nodes having a private key value associated therewith, the method comprising the computer-implemented steps of:

communicating a first public key value from a first node that is joining the first network communication entity to each other node that is currently within the first network communication entity (column 2, lines 20-44, column 8, line 30 to column 9, line 67);

receiving a collective public key value that is shared by each other node in the first network communication entity and that is based on private key values associated with each other node in the network communication entity (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67);

creating the group shared secret key value based on the collective public key value and the private key value associated with the first node (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67); and

joining the first node to a second network communication entity that includes the first network communication entity and the first node and that uses secure communication with messages that are encrypted using the group shared secret key value (column 4, lines 33-53, column 14, line 3 to column 16, line 58)

9. Regarding claim 12, Aziz teaches wherein joining the first node to a second network communication entity includes the step of communicating the first private key value to the second node and to the third node using messages encrypted using the shared secret key value (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58, i.e. acquiring a new member to join group).

10. Regarding claim 13, Aziz teaches wherein creating and storing a shared secret key value further comprises creating and storing the shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity (column 3, lines 9-50).

11. Regarding claim 14, Aziz teaches further comprising the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

12. With regards to claim 15, Aziz teaches wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation (column 3, lines 10-50, column 10, lines 3-40).

13. Regarding claim 17, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises creating and storing a subsequent collective public key based upon the collective public key value and the first public key value of the first node (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

14. Regarding claim 18, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises receiving the collective public key from one of the nodes of the first network communication entity that was the first node to join the first network communication entity (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

15. Regarding claim 19, Aziz teaches wherein creating and storing an initial shared secret key for the first node and second node comprises creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}{}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value (column 3, lines 10-50, column 10, lines 3-40).

16. As per claim 20, Aziz discloses a method for exchanging cryptographic keys, the method comprising:

forming a multicast group initially comprising a first node and a second node, the first node generating a first private value, the second node generating a second private value, wherein the initial multicast group exchanges the first private value and the second private value with ht second node and the first node, respectively, using a shard secret key, the multicast group generating a common public key (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67); and

joining the multicast group by a new node, the new node generating a new private value and a corresponding public key, the step of joining includes:

sending the common public key of the multicast group by a member of the multicast group by a member of the multicast group to the new node; tracking a number of times each node in the multicast group participates in the step of joining; computing a new shared secret key by the new node based upon the common public key of the multicast group and the new private value; publishing the public key of the new node; and computing the new shared secret key by each member of the multicast group based upon the public key of the new node, the private values of each member, and the number of times each node in the multicast group participates in the step of joining (column 4, lines 33-53, column 14, line 3 to column 16, line 58).

17. Concerning claim 22, Aziz discloses wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity (column 4, lines 33-53, column 14, line 3 to column 16, line 58).

18. Concerning claim 23, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric (column 12, line 59 to column 13, line 67).

19. Regarding claim 24, Aziz teaches wherein the plurality of nodes communicate over a packet switched network that supports, in part, Internet Protocol (column 2, lines 65-67).

20. Regarding claim 25, Aziz teaches wherein the first node, the second node, and the new node are authenticated by a distributed directory (column 4, lines 33-57).

21. Claims 16 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of U.S. Patent No. 6,629,243 to Kleinman et al, hereinafter Kleinman.

22. Regarding claims 16 and 21, Aziz does not teach wherein the step of communicating the first public key value of the first node to the first network communication entity by storing the first key value in a key distribution center.

23. Kleinman discloses wherein the step of communicating the first public key value of the first node to the first network communication entity by storing the first key value in a key distribution center (column 2, lines 60-67).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to distribute the keys via a key distribution center, since Kleinman states at column 2,

lines 51-59 that such a modification would ensure the safe and secure distribution of the keys to the respective members of the group.

Allowable Subject Matter

25. The following is a statement of reasons for the indication of allowable subject matter:

The Examiner could find no teachings in the prior art receiving a third public key valued from a third node that seeks to join the first network communication entity and creating a second shared secret key valued based on the collective public key value and the third public key value. Since no teachings or motivation can be found of receiving a third public key valued from a third node that seeks to join the first network communication entity and creating a second shared secret key valued based on the collective public key value and the third public key value, claims 1-10 and 26-28 are therefore novel and non-obvious.

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

27. The following patents are cited to further show the state of the art with respect to the closest related, commonly assigned, common inventor art, such as:

United States Patent No. 6,684,331 to Srivastava.

United States Patent No. 6,901,510 to Srivastava.

United States Patent No. 6,987,855 to Srivastava.

28. The following patents are cited to further show the state of the art with respect to similar methods as to the claimed invention, such as:

United States Patent No. 5,666,415 to Kaufman, which is to show user authentication.

United States Patent No. 5,491,750 to Bellare et al., which is to show three-party entity authentication and key distribution.

United States Patent No. 6,917,685 to Watanabe et al., which is to show IP key management.

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

31. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

CLF
Primary Examiner
AU 2131
1/22/06